Original Article

Available online at
www.bpasjournals.com

Bulletin of Pure and Applied Sciences.
Vol. 38E (Math & Stat.), No.1, 2019. P.155-158
Print version ISSN 0970 6577
Online version ISSN 2320 3226
DOI: 10.5958/2320-3226.2019.00013.4

SYMMETRY GROUPS OF SOME HADAMARD MATRICES

N.V. Ramana Murty[1,*], G.M. Victor Emmanuel[2], P. Venu Gopala Rao[3], M. Maria Das[4]

Author Affiliation:
[1]Department of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh 520008, India
E-mail: raman93in@gmail.com
[2]Department of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh 520008, India
E-mail: gmvictorsj@gmail.com
[3]Department of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh 520008, India
E-mail: venugopalparuchuri@gmail.com
[4]Department of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh 520008, India
E-mail: mariadas197475@gmail.com

***Corresponding Author:**
N.V. Ramana Murty, Department of Mathematics, Andhra Loyola College, Vijayawada, Andhra Pradesh 520008, India
E-mail: raman93in@gmail.com

Received on 04.12.2018, Revised on 19.02.2019 Accepted on 20.03.2019

Abstract: Hadamard matrices are a special class of square matrices with entries 1 and -1 only. They have many applications in Coding Theory, Physics, Chemistry and Neural networks. Therefore, this paper makes an attempt to study Hadamard matrices and their connection with Group Theory. Especially, we concentrate on the Symmetry groups of Standard Hadamard matrices H_0, H_1, H_2, H_3 and H_4. It is shown that the Symmetry group of the Standard Hadamard matrices H_0 and H_1 is the trivial group and that of H_2 is isomorphic to the Permutation group S_3. Since Symmetry group of the Standard Hadamard matrix H_n is isomorphic to the General linear group of $n \times n$ invertible matrices over the field $\mathbb{Z}_2$ and the order of the General linear group $GL(n,q)$ of $n \times n$ invertible matrices over a finite field F containing q elements is $\prod_{k=0}^{n-1}\left(q^n - q^k\right) = \left(q^n - q^0\right)\left(q^n - q^1\right)\left(q^n - q^2\right)\cdots\left(q^n - q^{n-1}\right)$, it is shown that the orders of the Symmetry groups of H_3 and H_4 are 168 and 20,160 respectively.

1. INTRODUCTION

The name Hadamard matrix came after the name of Jacques Hadamard, a French mathematician. A Hadamard matrix H of order $n \times n$ is a matrix with entries 1 and -1 such that $H^T H = HH^T = nI_n$, where H^T is the transpose of H and I_n is the Identity matrix of order n. This means that the dot product of any two distinct rows or columns of H is equal to zero. That is, any two distinct rows or columns are orthogonal. Hadamard matrix is non-singular and the determinant of the Hadamard matrix of order n is $n^{n/2}$. Symmetric Hadamard matrices are known as Standard Hadamard matrices, and they are denoted by $H_0, H_1, H_2, \cdots$, where H_0 is of order 1×1, H_1 is of order 2×2, H_2 is of order 4×4, H_3 is of order 8×8, and so on.

That is, $H_0=(1)$, $H_1=\begin{bmatrix} H_0 & H_0 \\ H_0 & -H_0 \end{bmatrix}, H_2=\begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix}, H_3=\begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix}$ and so on. The Hadamard matrices $H_0, H_1, H_2, H_3, \cdots$ are known as 'Standard Hadamard matrices'. From these examples, it is easy to see that Standard Hadamard matrix H_n is a square matrix of order 2^n. There are many ways to construct these matrices among which Payley's construction is one of the interesting methods. As we are concentrating on group actions, construction methods are not discussed here.

2. MAIN RESULTS

Definition 2.1: Each row h_i of a Hadamard matrix is called a 'Hadamard pattern' and the set of all Hadamard patterns of the Hadamard matrix H is denoted by $P(H)$.

Example 1: The second row 1, -1, 1, -1 of the matrix H_2 is a Hadamard pattern.

Definition 2.2: The Hadamard pattern set $P(H)$ of the rows $h_1, h_2, \cdots, h_n$ of H is known as a 'Hadamard network'.

Example 2: The Hadamard network of the matrix H_2 is given by $P(H_2)=\{h_1,h_2,h_3,h_4\}$, where $h_1=(1,1,1,1), h_2=(1,-1,1,-1), h_3=(1,1,-1,-1), h_4=(1,-1,-1,1)$.

Definition 2.3: If α is a permutation in the Permutation group S_k, then it induces a mapping $\tilde{\alpha}: P(H) \to P(H)$ of the corresponding states defined by $\tilde{\alpha}(s_1,s_2,\cdots,s_k)=\left(s_{\alpha(1)},s_{\alpha(2)},\cdots,s_{\alpha(k)}\right)$.

Example 3: If $\alpha=(3,4)\in S_4$ then it gives $\tilde{\alpha}(s_1,s_2,s_3,s_4)=(s_1,s_2,s_4,s_3)$ which induces for $h_2=(1,-1,1,-1)$ in $P(H_2)$, $\tilde{\alpha}(1,-1,1,-1)=(1,-1,-1,1)$.

Definition 2.4: If H be a Hadamard matrix of order k with Hadamard network $P(H)=\{h_1,h_2,\cdots,h_n\}$, then α belongs to the set $S(H)$, known as the set of Symmetries of the standard Hadamard matrix H, if $\tilde{\alpha}(h_i)=h_j, \forall h_i \in P(H), 1\le i,j\le k,$ where S_k is the Permutation group on k symbols.

Example 4: If $\alpha=(2,3)$ be a permutation in S_4 and the Hadamard network of the Standard Hadamard matrix H_2 be $P(H_2)=\{h_1=(1,1,1,1),h_2=(1,-1,1,-1),h_3=(1,1,-1,-1),h_4=(1,-1,-1,1)\}$, then $\tilde{\alpha}(h_1)=h_1, \tilde{\alpha}(h_2)=h_3, \tilde{\alpha}(h_3)=h_2, \alpha(h_4)=h_4$. Therefore, $\alpha\in S(H_2)$. But, the permutation $(1,3)$ does not belong to $S(H_2)$ since $\tilde{\alpha}(h_3)=(-1,1,1,-1)\notin P(H_2)$.

Theorem 2.5: The set of Symmetries $S(H)$ of the Hadamard matrix H of order k forms a group with respect to the composition of the permutations defined in the Permutation group S_k.

Proof: If $\alpha,\beta\in S(H), \tilde{\alpha}(h_i)=h_j, \tilde{\beta}(h_i)=h_t, \forall h_i\in P(H)$. Therefore $(\tilde{\alpha}\circ\tilde{\beta})(h_i)=\tilde{\alpha}(\tilde{\beta}(h_i))=\tilde{\alpha}(h_t)=h_r \Rightarrow (\tilde{\alpha}\circ\tilde{\beta})\in P(H)\Rightarrow \alpha\circ\beta\in S(H)$. Since the composition of permutations is associative, obviously $S(H)$ satisfies the Associative Law, and since Identity permutation I in S_k induces Identity map on $P(H)$, it is clear that $I\in S(H)$ and $(\alpha\circ I)=(I\circ\alpha)=\alpha, \forall \alpha\in S(H)$. It is easy to see that $\tilde{\alpha}: P(H)\to P(H)$ is one-one and onto. Therefore, $(\tilde{\alpha})^{-1}$ is defined on $P(H)$, and hence $\alpha^{-1}\in S(H)$ such that $\alpha\circ\alpha^{-1}=I$. Hence, $S(H)$ forms a group.

Remark: Since the composition of permutations is not commutative, the group $S(H)$ is not abelian.

3. SYMMETRY GROUPS OF H_0, H_1, H_2, H_3

If H_n is a Standard Hadamard matrix, it has 2^n elements, and each element of $P(H)$ begins with 1. Therefore, each $\tilde{\alpha} \in S(H)$ has $\alpha(1) = 1$. Hence, the Symmetry group $S(H_0)$ of the first Standard Hadamard matrix H_0 is the trivial group. That is, $S(H_0) = \{I\}$, where I is the identity element.

For the second Standard Hadamard matrix H_1, the pattern set is $P(H_1) = \{h_1 = (1,1), h_2 = (1,-1)\}$. Since H_1 is a square matrix of order 2, consider the Permutation group $S_2 = \{I, (1,2)\}$ on 2 symbols. The identity permutation I induces $\tilde{I}(h_1) = h_1$ and $\tilde{I}(h_2) = h_2$ and hence $I \in S(H_1)$. If $\alpha = (1,2)$, then $\tilde{\alpha}(1,2) = (2,1)$ and hence $\tilde{\alpha}(h_1) = h_1$ and $\tilde{\alpha}(h_2) = (-1,1) \notin P(H_2)$. Therefore, the permutation $(1,2) \notin S(H_1)$. Hence, $S(H_1) = \{I\}$, the trivial group.

The Pattern set $P(H_2)$ of the Standard Hadamard matrix H_2 is $P(H_2) = \{h_1 = (1,1,1,1), h_2 = (1,-1,1,-1), h_3 = (1,1,-1,-1), h_4 = (1,-1,-1,1)\}$. Since H_2 is a square matrix of order 4, consider the Permutation group S_4 whose order is 24. Since the first entry of each pattern of H_2 begins with 1, out of 24 permutations of the group S_4, the permutations in which the first element does not change shall belong to the Symmetry group $S(H_2)$. That is, the permutations α in which $\alpha(1) = 1$ belongs to $S(H_2)$. Therefore, $S(H_2) = \{I, (2,3), (2,4), (3,4), (2,3,4), (2,4,3)\}$, contains six elements among which 3 are even permutations and 3 are odd. Therefore, it is easy to see that the Symmetry group $S(H_2)$ is isomorphic to the Permutation group S_3. That is, $S(H_2) \cong S_3$.

Before going to the fourth Standard Hadamard matrix H_3, it is necessary to go through the following theorems.

Theorem 2.6: For the Standard Hadamard matrices, H_n, the Symmetry group $S(H_n)$ is isomorphic to the General linear group of $n \times n$ invertible matrices over the field $\mathbb{Z}_2$. That is, $S(H_n) \cong GL(n, \mathbb{Z}_2)$.

Proof: See [1].

Theorem 2.7: The order of the General linear group $GL(n,q)$ of $n \times n$ invertible matrices over a finite field F containing q elements is $\prod_{k=0}^{n-1}(q^n - q^k) = (q^n - q^0)(q^n - q^1)(q^n - q^2)\cdots(q^n - q^{n-1})$.

Proof: See [2].

Therefore, by the Theorems 2.6 and 2.7, for the fourth Standard Hadamard matrix H_3, we have $S(H_3) \cong GL(3, \mathbb{Z}_2) \Rightarrow |S(H_3)| = |GL(3, |\mathbb{Z}_2|)| \Rightarrow |S(H_3)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$, since $|\mathbb{Z}_2| = 2$. Similarly, for the fifth Standard Hadamard matrix $S(H_4)$, it is obvious to see that

$$S(H_4) \cong GL(4, \mathbb{Z}_2) \Rightarrow |S(H_4)| = |GL(4, |\mathbb{Z}_2|)|$$
$$\Rightarrow |S(H_4)| = (2^4 - 1)(2^4 - 2^1)(2^4 - 2^2)(2^4 - 2^3) = (15)(14)(12)(8) = 20{,}160.$$

Remark: It is clear that the group $S(H_3)$ is a subgroup of the Permutation group S_8 on 8 symbols, and $S(H_4)$ is a subgroup of the Permutation group S_{16} on 16 symbols.

REFERENCES

[1]. Folk, R., Karatashov, A., Linsonek, P. and Paule, P. (1993). Symmetries in Neural Networks: A Linear Group Action Approach, *J. Phys. A.Math. Gen.*, 26, 3159-3164.
[2]. Lanski, Charles (2004). Concepts in Abstract Algebra, Cengage Learning Inc., Florence, KY, U.S.
[3]. Dummit, David S. and Foote, Richard M. (2005). Abstract Algebra, John Wiley and Sons, New York.
[4]. Cohn, P.M. (2004). Further Algebra and Applications, Springer.